Amendments to the Claims:

This listing of claims will replace all prior versions, and listings of claims in the application:

Listing of Claims:

1. (Original) In a network device having a plurality of ports and providing switching functions between ports, a method for providing port security, comprising:

receiving a first data packet on a port;

determining a first MAC address for the received first data packet;

determining a first source IP address for the received first data packet, wherein the first source IP address for the received first data packet and the first MAC address for the received first data packet form a first source IP address and MAC address pair;

comparing the first source IP address and MAC address pair with information in a table which stores source IP address and MAC address pairs; and

passing the received first data packet through the port, when the first source IP address and MAC address pair is found in the table.

2. (Original) The method of claim 1 further comprising:

receiving a second data packet on the port;

determining if a second MAC address for second data packet is a new MAC address;

when the second MAC address for the received second data packet is determined to be a new MAC address, learning the source IP address for the second MAC address, wherein the second MAC address and the learned source IP address form a second IP address and MAC address pair; and

storing the second IP address and MAC address pair in the table.

3. (Original) The method of claim 2 further comprising:

performing a reverse IP check to confirm the learned source IP address.

4. (Original) The method of claim 1 further comprising:

determining if a second MAC address for a second received data packet is a new MAC address;

wherein when the second MAC address for the second received data packet is determined to be a new MAC address, learning the source IP address for the second MAC address, wherein the second MAC address and the learned source IP address form a second IP address and MAC address pair, wherein the learning of the source IP address utilizes at least one of the processes selected from the following group of processes: (1) using a reverse address resolution protocol; (2) listening to a DHCP response packet; (3) watching for a IP header information in a data packet; and (4) listening to ARP requests and ARP reply messages; and

storing the second IP address and MAC address pair in the table.

5. (Original) The method of claim 2 wherein the table is stored in an access control list of a content addressable memory device.

6. (Currently Amended) The method of claim 1 further comprising:

detecting when a device having a second source IP address, which is stored in the table, is no longer ~~present on~~ coupled to the port; and

removing the second source IP address from the table when the device having the second source IP address is determined to no longer be ~~present on~~ coupled to the port.

7. (Currently Amended) The method of claim 2 further comprising:

detecting when a device having the learned source IP address, which is stored in the table, is no longer ~~present on~~ coupled to the port; and

removing the learned source IP address from the table when the device having the learned source IP address is determined to no longer be ~~present on~~ coupled to the port.

8. (Original) The method of claim 1 further comprising receiving input from a system administrator which selects a maximum number of source IP addresses which have access through a port.

9. (Original) The method of claim 1 further comprising receiving input from a system administrator which selects ports of the plurality of ports, where access though selected ports will be provided based on a source IP address and MAC address pair contained in a data packet.

10. (Canceled)

11. (Currently Amended) The method of claim [[10]] 1 further comprising:

receiving a second data packet on the port; and

blocking the second data packet at the port, if ~~the~~ a second source IP address and a second MAC address for the second data packet is determined to not be stored in the table, and a maximum number of source IP addresses ~~are~~ already [[on]] have access through the port.

12. (Currently Amended) The method of claim [[10]] 1 further comprising:

receiving a second data packet on the port;

determining ~~the~~ a second source IP address and a second MAC address for the second data packet; and

storing the second source IP address and the second MAC address in the table, if a maximum number of source IP addresses has not already been reached for the port, and passing the second data packet through the port.

13. (Currently Amended) The method of claim 12 further comprising blocking the second data packet at the port, when the source IP address for the second data packet is determined to not be stored in the table, and a maximum number of source IP addresses ~~are~~ already [[on]] have access through the port.

14 - 16. (Canceled)

17. (Currently Amended) A network device for use in a computer network having a plurality of hosts each host having a MAC address, the network device comprising:

a plurality of ports;

a MAC detector which operates to identify a source MAC address for a ~~first host coupled to~~ data packet received at a first port of the plurality of ports;

a source IP address detector which operates to identify a source IP address for ~~the first host~~ the data packet, wherein the source IP address for the data packet and the source MAC address for the data packet form a source IP address and MAC address pair; and

a processor which operates to: ~~associate the source IP address with the MAC address for the first host, and based on the association of the first source IP address with first MAC address, the processor operates to control the first host's access to the computer network through the first port.~~

compare the source IP address and MAC address pair with information in a table which stores a plurality of source IP address and MAC address pairs; and

pass the data packet through the first port when the source IP address and MAC address pair is found in the table.

18. (Currently Amended) The network device of claim 17 wherein the processor includes a content addressable memory and wherein the table is stored in an access control list of the content addressable memory ~~includes an access control list which associates the MAC address with the source IP address for the first host, and the content addressable memory is programmed to allow the first host access through the first port when the content addressable memory determines that data packets from the first host identify the data packets as coming from the first host having the MAC address and the source IP address~~.

19. (Canceled)

20. (Currently Amended) The network device of claim 17 wherein the processor ~~determines that the first host is sending data packets which do not contain both the MAC address and the source IP address previously learned, the processor operates to deny the first host access through the first port~~ further operates to block the data packet at the first port when the source IP address and MAC address pair is not found in the table.

21. (Currently Amended) The network device of claim 17 wherein the processor ~~can~~ further ~~operate~~ operates to selectively block access to selected ports of the plurality of ports based on a source IP address contained in data packets received at a port.

22. (New) A method for providing port security in a network device, the method comprising:

comparing a first source IP address and MAC address pair with a plurality of source IP address and MAC address pairs stored in a table of the network device, the first source IP address and MAC address pair being determined from a data packet received at a port of the network device;

if the first source IP address and MAC address pair is found in the table, passing the data packet through the port; and

if the first source IP address and MAC address pair is not found in the table, blocking the data packet at the port.